The Survivable Network Analysis Method:

Assessing Survivability of Critical Systems

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Sponsored by the U.S. Department of Defense

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2000		**00-00-2000 to 00-00-2000**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Survivable Network Analysis Method: Assessing Survivability of Critical Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**42**	

Agenda

System Survivability Concepts

The Survivable Network Analysis (SNA) Method

System Survivability Concepts

Survivability Motivation

Growing societal dependence on complex, large-scale, networked systems

Serious consequences of system compromises and failures

Traditional security and vulnerability analysis no longer sufficient

Changing Systems Environment

System evolution

- **expanding network boundaries**
- **additional participants with varying levels of trust**
- **numerous point solutions: Public Key Infrastructure, Virtual Private Networks, firewalls, ...**
- **blurring of Intranet and Extranet boundaries**
- **new technologies -- directory services, XML**

System security

- **No amount of security can guarantee a system will not be penetrated**

Impact on Analysis

Lack of complete information

- **unknown physical and logical perimeters**
- **unknown participants, untrusted insiders**
- **unknown software components -- COTS, Java, etc.**

Broader scope

- **Mix of central and local administrative control**
- **Critical components more exposed**
- **Attacks can impact essential business services**

From Security to Survivability

Survivability focus is on the system mission

- **assume imperfect defenses**
- **analyze mission risks and tradeoffs**
- **identify decision points with survivability impact**
- **provide recommendations with business justification**
- **improve survivability to ensure mission capability**

Survivability **is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.**

The “Three Rs” of Survivability

Resistance
- **capability to deter attacks**

Recognition
- **capability to recognize attacks and extent of damage**

Recovery
- **capability to provide essential services and assets during attack and recover full services after attack**

The Survivable Network Analysis (SNA) Method

SNA Objectives

Understand survivability risks to a system

- **What essential services must survive intrusions?**
- **What are the effects of intrusions on the mission?**

Identify mitigating strategies

- **What process, requirements, or architecture changes can improve survivability?**
- **Which changes have the highest payoff?**

SNA Characteristics

Tailorable to stage of development -- from initial requirements to deployed systems

Adaptable to variety of development processes

Applies to applications as well as infrastructure

SNA Architecture Focus

Architecture is integrating element of large systems

Capture assumptions on boundaries and users

Support architecture evolution as requirements and technologies change

- **evolving functional requirements**
- **trend to loosely coupled systems**
- **integration across diverse systems**
- **changes in vendor product architectures**

Assist selection and integration of rapidly changing security products

The SNA Process

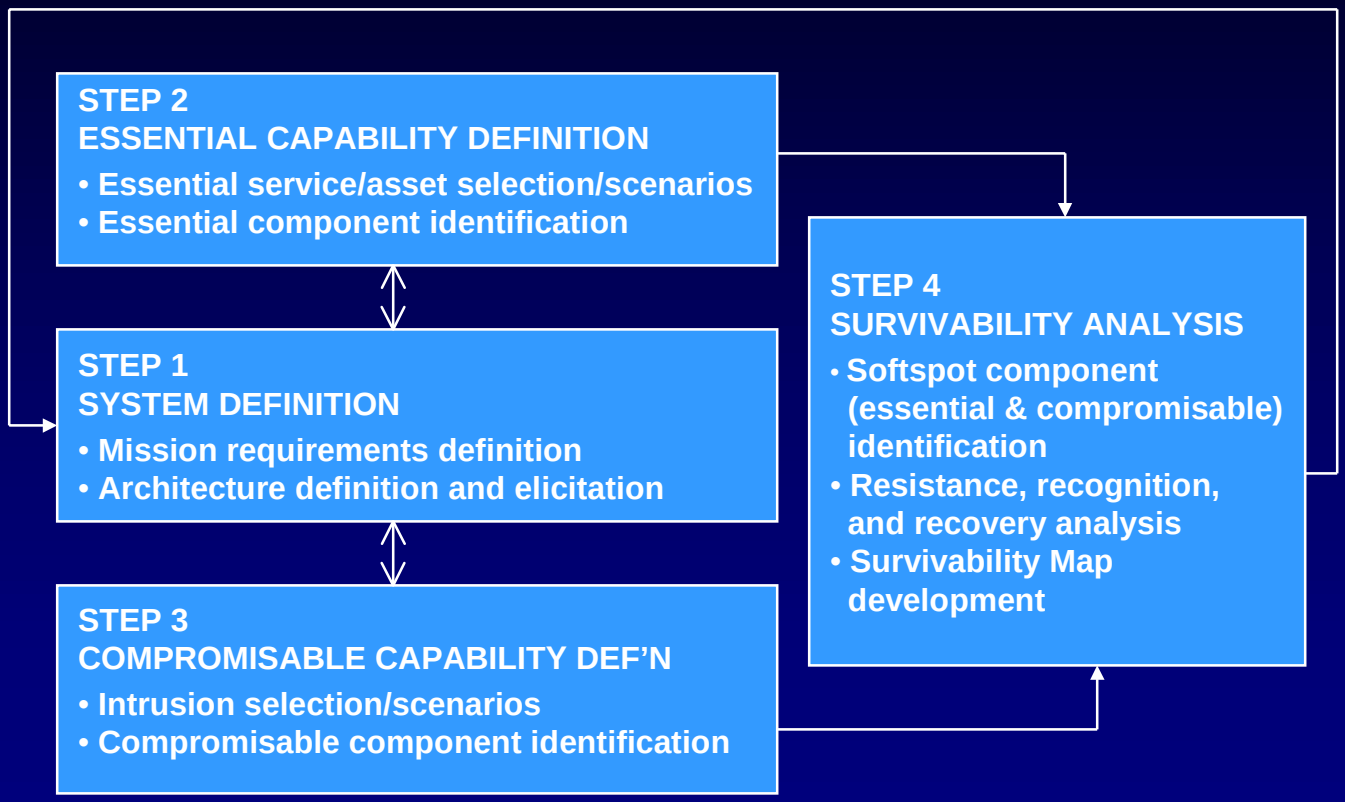
Performed on selected system or system component

Conducted by our team (survivability expertise) working with customer team (system expertise)

Carried out in structured series of working sessions

Findings summarized in report and management briefing

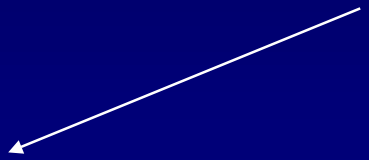
Survivable Network Analysis Method



SNA Preliminaries - 1

Joint Planning Meeting/System Documentation
Identify system to be analyzed and documentation
Establish scope of work, teams, and schedules

Off-Site Preparation Task
Review system documentation
Prepare for SNA



Joint Discovery Session

...

SNA Preliminaries - 2

Existing documentation may only partially meet SNA needs

System architecture description may be little more than boxes and arrows

Discovery sessions will continually add new components and functionality to architecture

Critical to have stakeholder involvement and interest

Step 1 and 2 Activities

Joint Discovery Session

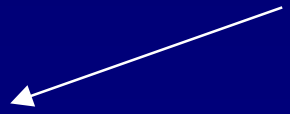
SNA Step 1 initiation:
- Briefings by developers on
  - business mission and life-cycle process
  - functional requirements
  - operating environment
  - architecture
  - evolution plans

SNA Step 2 initiation:
- Determination of
  - essential service and asset selection
  - essential service/asset usage scenarios
  - scenario traces and essential components

Off-site Discovery Integration Task

SNA Steps 1 and 2 completion:
- Analyze system mission, life cycle, requirements, environment, architecture and essential services, assets, and components

SNA Step 3 initiation:
- Assess system vulnerabilities
- Define representative set of intrusions
- Define intrusion usage scenarios



Joint Discovery Session

...

Step 1: Mission Definition

Inputs required from diverse stakeholders

- **owners, users, architects, developers, administrators**

Identify business mission supported by the system

- **example**
  - **government agency: review, select, fund, and monitor government contracts**
- **example**
  - **industry: support integration of design teams across internal corporate organization, industry partners, and contractors**

Step 1: Architecture Definition

System architecture and operating environment

- **evaluation team reviews understanding of architecture from documentation and discussion**
- **review key system boundaries such as where administrative control changes**
  - **risks may be with external systems or with systems outside immediate control of the organization**
- **identify explicit and implicit assumptions such as choice of vendors, operating systems**
- **identify critical dependencies on other systems**

Step 2: Essential Capabilities

Essential services/assets

- **Capabilities that must be available despite intrusions**

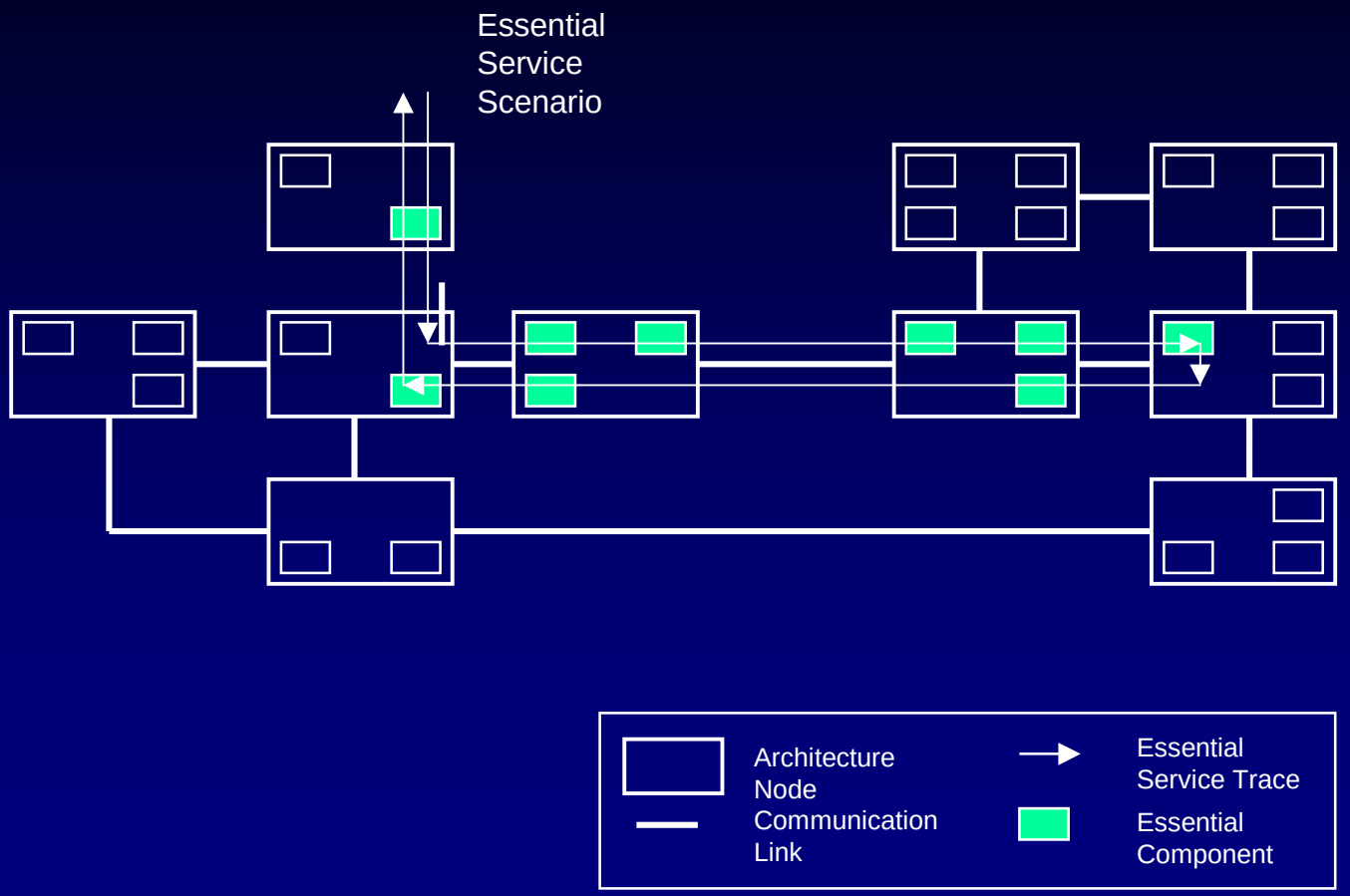
Essential service/asset scenarios

- **Steps in essential service/asset usage**

Essential components

- **Architecture parts required by essential services/assets**
- **Determined by tracing scenarios through architecture**

Essential Service Scenario Trace



Step 2: Essential Services

Ask user communities to describe their system use

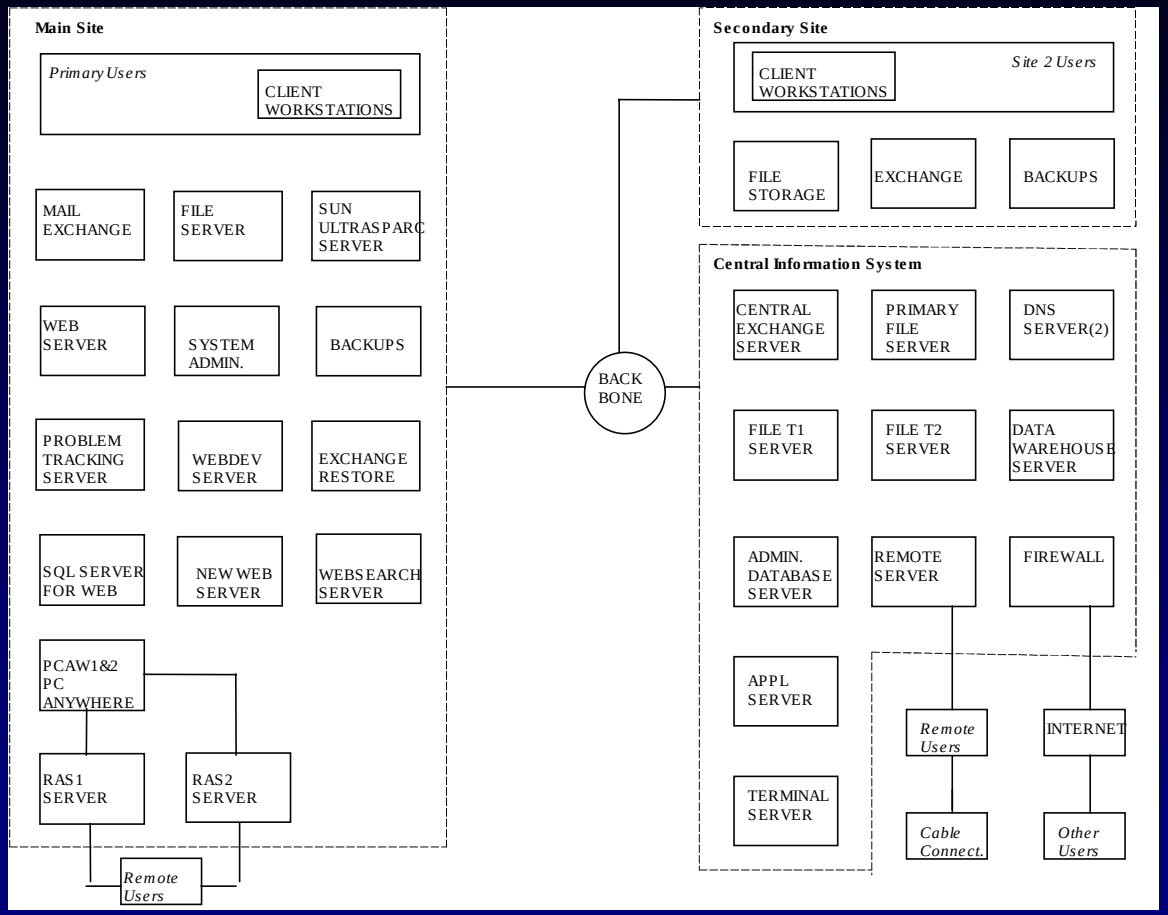
- **government agency: file system was essential component but users employed email servers as an alternative file system with extensive storage of attachments**

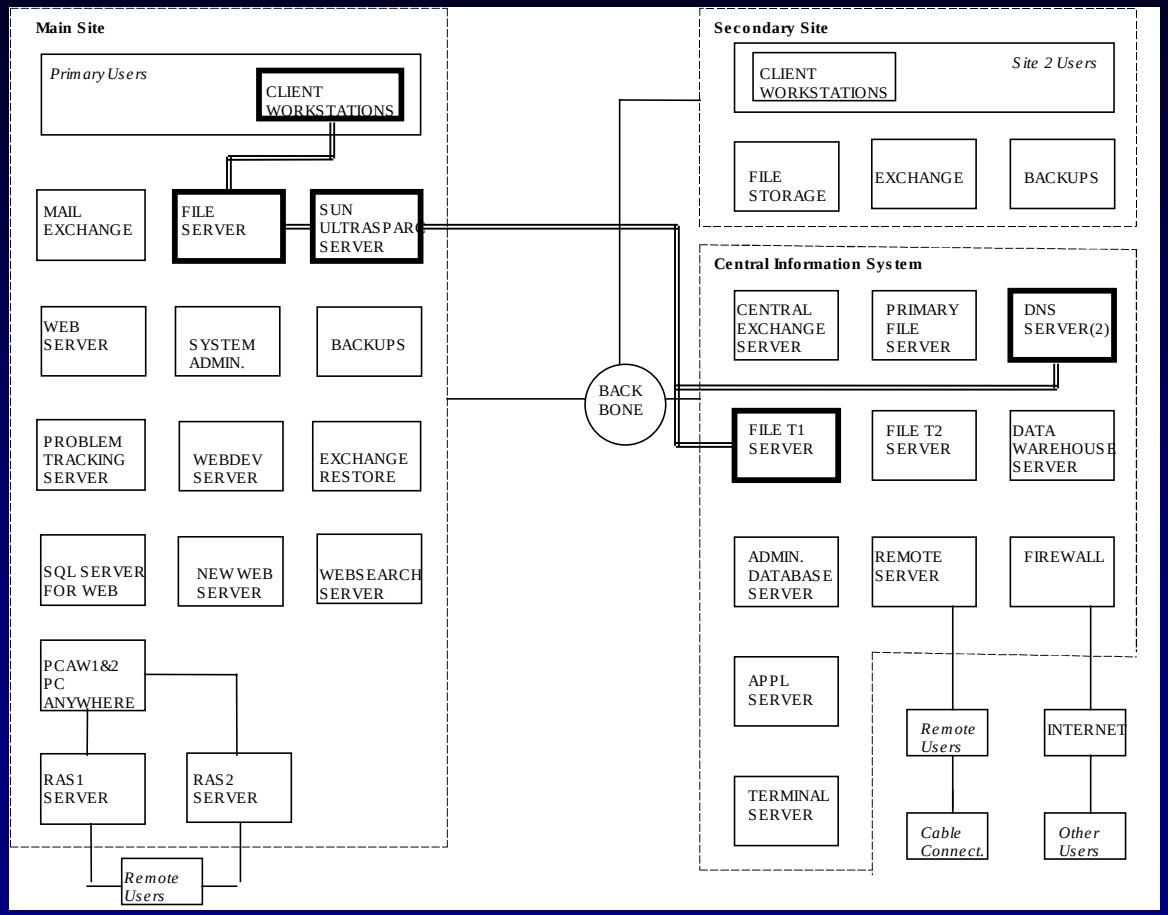
Identify future changes in function and usage

- **government agency: electronic submission of grant proposals and financial reports**

Identify small number of essential services

- **government agency: grant administration, internal administration, dissemination of public information**


Main Site
Primary Users
CLIENT WORKSTATIONS
MAIL EXCHANGE
FILE SERVER
SUN ULTRASPARC SERVER
WEB SERVER
SYSTEM ADMIN.
BACKUPS
PROBLEM TRACKING SERVER
WEBDEV SERVER
EXCHANGE RESTORE
SQL SERVER FOR WEB
NEW WEB SERVER
WEBSEARCH SERVER
PCAW1&2 PC ANYWHERE
RAS1 SERVER
RAS2 SERVER
Remote Users
BACK BONE
Secondary Site
CLIENT WORKSTATIONS
Site 2 Users
FILE STORAGE
EXCHANGE
BACKUPS
Central Information System
CENTRAL EXCHANGE SERVER
PRIMARY FILE SERVER
DNS SERVER(2)
FILE T1 SERVER
FILE T2 SERVER
DATA WAREHOUSE SERVER
ADMIN. DATABASE SERVER
REMOTE SERVER
FIREWALL
APPL SERVER
TERMINAL SERVER
Remote Users
INTERNET
Cable Connect.
Other Users

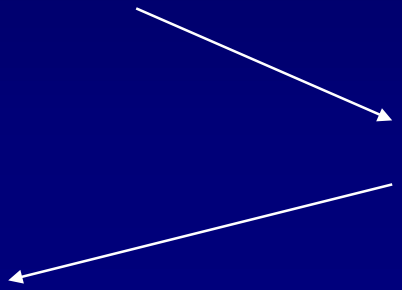


Step 3 and 4 Activities

Joint Analysis Session

SNA Step 3 completion:
- Briefing by SEI on
  - system vulnerabilities
  - selected intrusions and their usage scenarios
- Validation of intrusions by customer team
- Determination of
  - scenario traces/compromisable components

SNA Step 4 initiation:
- Determination of
  - softspot components
  - current resistance, recognition, and recovery



Off-site Analysis Integration Task

SNA Step 4 completion:
- Define recommended mitigation strategies for resistance, recognition, and recovery
- Assess architecture modifications and impacts
- Document findings in the Survivability Map
- Prepare customer briefing

Briefing

Step 3: Intrusion Capabilities

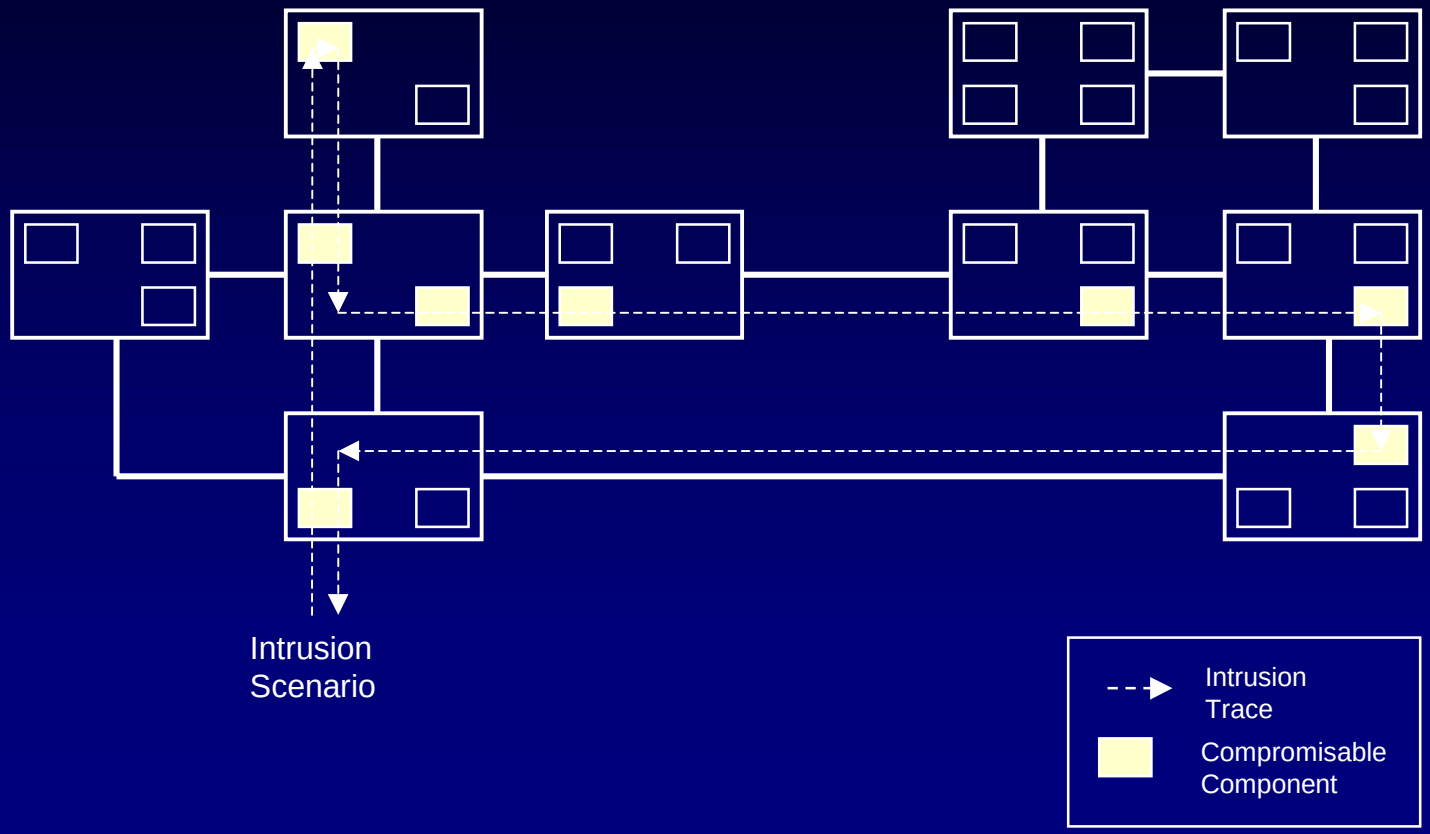
Treat intruders as users

Select representative intrusions based on environment and risk

Intrusion scenarios
- **steps in attacker usage**

Compromisable components
- **architecture parts accessible by intrusion scenarios**
- **determined by tracing scenarios through architecture**

Intrusion Scenario Trace



Step 3: Vulnerabilities

Review initial analysis of probable attacks and impacts with stakeholders and users

- **often significant variation in stakeholder view of intruder impact**
- **script-kiddie attackers generate most attention but may draw focus away from skilled attackers with specific objectives**
- **generate stakeholder consensus on probable attackers and impacts**

Step 3: Model Attacker Profiles - 1

"Target of opportunity" profile -- general objectives
- **readily available tools**
- **defense: increased resistance, system configurations, file-integrity checks**

"Intermediate" profile -- specific objectives
- **use of trusted resources, greater patience**
- **higher impact on essential services**
- **defense: increased recognition and recovery**

"Sophisticated" profile -- very focused objectives
- **customized tools, compromise internal staff**
- **defense: high probability of success; recognition and recovery essential**

Step 3: Model Attacker Profiles - 2

Generate table of probable attackers and impacts

For each class of attacker consider

- **resources:** personnel, skill, finances
- **time:** patience and persistence
- **tools:** access to tools, ability to customize
- **risk:** level of risk aversion
- **access:** internal, Internet
- **objectives:** personnel, financial, moral

Example: Government agencies may have attackers who have strong political or moral positions. These attackers are not risk averse and can be very patient.

Step 3: Current Strategies

Identify current survivability strategies

- **normal operations for backup**
- **configuration management**
- **resistance, recognition, recovery (usually weak)**

Get input from users, management, and system administrators

Step 4: Survivability Analysis

Steps 1-3 provide information for extensive, in-depth analysis to develop recommendations for

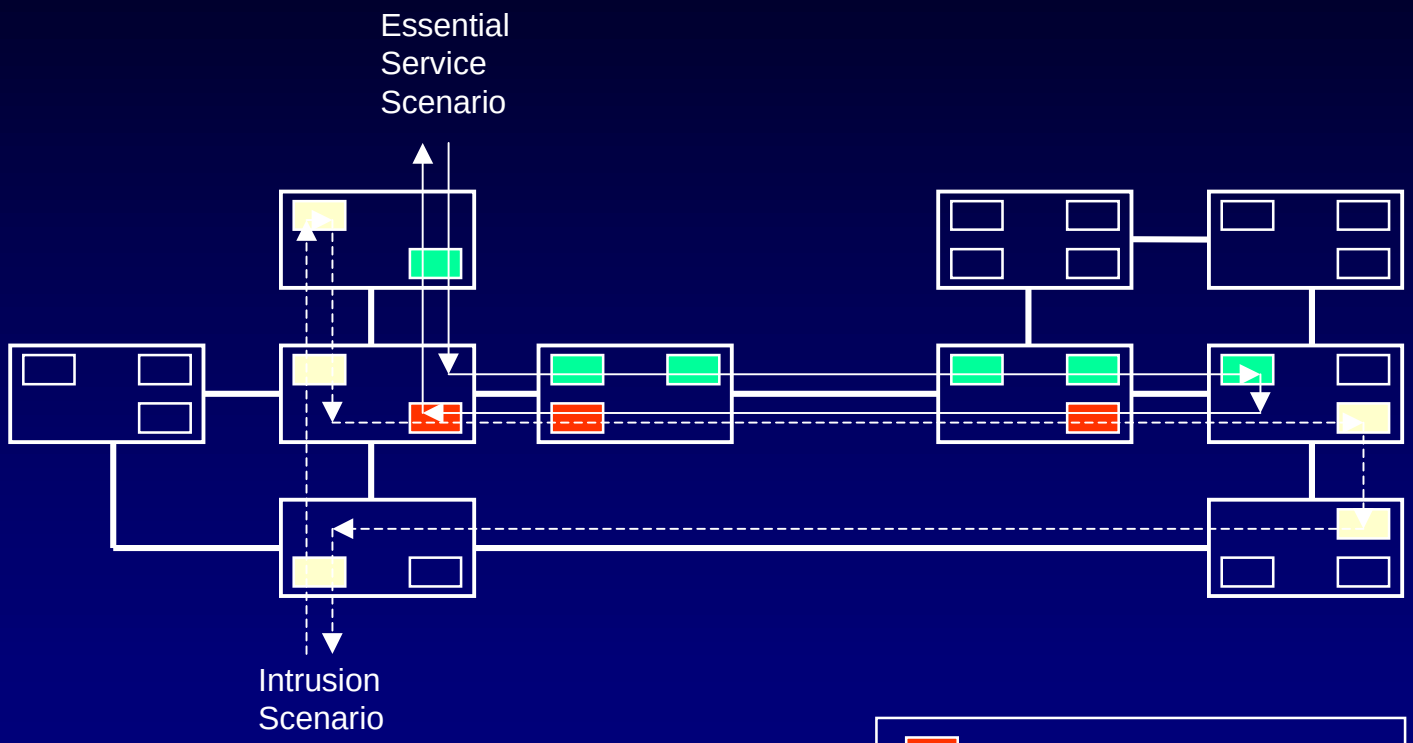
- **architecture modifications**
- **requirements changes**
- **policy revisions**
- **operational improvements**

Step 4: Softspot Identification

Softspot components

- **architecture components that are both essential and compromisable**
- **members of essential service scenario traces that must be available despite intrusion effects**

Architecture Softspots



Step 4: Survivability Analysis

Evaluate system in terms of response to scenarios

Make recommendations for survivability improvements

- **requirements: propose response to intrusions**
- **architecture: evaluate system and operational behavior**

Identify decision and tradeoff points

- **areas of high risk**
- **tradeoffs with safety, reliability, performance, usability**

Step 4: Survivability Map

Defines survivability strategies for the three Rs based on intrusion softspots

Relates survivability strategies to the system, its environment, and identified intrusions

Provides basis for risk analysis, cost-benefit tradeoffs

SNA Survivability Map

Intrusion Scenario	Softspots	Architecture Strategies for →	Resistance	Recognition	Recovery
Scenario 1 ...		Current			
		Recommended			
Scenario n		Current			
		Recommended			

Step 4: Recommendations - 1

Case Study A: large distributed organization, large number of legacy systems, currently involved in redesign of most major systems

- **establish security architecture -- directory services, support for a mix of central and distributed administration, develop common application interface to security infrastructure, architectural support for managing active content (Javascript, email attachments)**
- **support architecture evolution -- accommodate product changes, interoperability among security vendors, and changes in vendor architecture**

Step 4: Recommendations - 2

Case Study B: administrative unit inside a large, diverse organization. Very heterogeneous user environment (university-like) including significant research component

- **revise security/survivability policies**
- **improve separation between internal systems and those accessed by general public and employees outside the administrative unit**
- **add internal firewalls to better manage diverse user community**
- **extend attacker analysis beyond script-kiddies**
- **improve system recovery**

SNA Benefits

Clarified requirements

Basis to evaluate changes in architecture

Early problem identification

Increased stakeholder communication

Improved system survivability

Future Work

Define survivability architecture patterns

Develop improved methods for system and intrusion definition

Create automation support for SNA

Additional Information

SNA Case Study: The Vigilant Healthcare System

- **IEEE Software: July/August 1999**

Survivability: Protecting Your Critical Systems

- **IEEE Internet Computing: November/December 1999**

Web site: IEEE article and other reports

On www.sei.cmu.edu
/organization/programs/nss/surv-net-tech.html